



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,823	12/05/2003	Steven Townsend	7344/15	8539
22801	7590	10/30/2007		
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			EXAMINER PARTHASARATHY, PRAMILA	
			ART UNIT	PAPER NUMBER
			2136	
			MAIL DATE	DELIVERY MODE
			10/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/729,823

Applicant(s)

TOWNSEND ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 August 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☒ Claim(s) 11 and 30 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>7/16/2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to the communication 8/23/2007. Claims 1 – 32 are currently pending.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, filed on 1/2/2007 is attached to the Office action.

Response to Arguments

3. Applicant's arguments filed July 16, 2007 have been fully considered:

Applicant states "Applicant respectfully requests that the provisional double-patenting rejections be held in abeyance until corresponding claims are indicated as allowable." and "In the event such claims from more than one application are indicated as allowable, Applicant agrees to submit a terminal disclaimer to overcome the provisional double-patenting rejection."

Examiner respectfully maintains the double patenting rejections as claims of copending application 10/456,093 are in fact, allowed (Notice of Allowance mailing date 9/26/2007) and requests the Applicant to file terminal disclaimer to overcome double patenting rejections.

Applicant's amendment to claims overcame 35 USC 101 rejections and Examiner hereby withdraws 35 USC 101 rejections.

Applicant's amendment to claims does not overcome 35 USC 112 rejections and Examiner hereby maintains these rejections. Examiner suggests defining "exposing" a

Art Unit: 2136

function in terms of “policy reader module”, API 124, or “security module that creates a new set of rules”.

4. Applicant mainly argues that Ko et al. (Patent 6,789,202) does not teach “readiness to implement the new security policy” and “identifying whether each of the plurality of security engines is prepared to apply the new security policy”. Examiner directs to instant specification paragraph [0083] wherein “readiness to implement the new set of security policy” implies that each security engine returns a value “ok” or value “fail” to indicate that it is ready to receive and begin using new set of rules.

Ko et al. discloses “Analyzer receives an instruction detection policy from higher level analyzer or a network security coordinator”, “Analysis module gathers and correlates information reported by sensors based on attacks specified in the intrusion detection policy for analyzer” and “The results generated by analysis module are sent to decision module which carries out the appropriate response based upon the given intrusion detection policy” (See column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter broadly recited in the amended independent claims. The dependent claims are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims is respectfully maintained.

Examiner withdraws prior art rejection for dependent Claims 11 and 30 (please refer to Allowable subject matter, section 38).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1 – 32 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 5, 8 – 17 and 19 – 32 of copending Application No. 10/729,096. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 32 correspond to the claims of 1 – 5, 8 – 17 and 19 – 32 of the copending application claims, except in the instant claims element "communicates new data associated with an existing security policy", is referred in the copending application claims as "communicating ... a password that does not comply with predetermined criteria". It would have been obvious to one having ordinary skill in the art to recognize that communicating new data and associating it with an existing

Art Unit: 2136

security policy is equivalent to identifying and communicating that the password does not comply with the predetermined (existing) criteria (security policy).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

6. Claims 1 – 32 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 53 of copending Application No. 10/729,530. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 32 correspond to the claims of 1 – 53 of the copending application claims, except in the instant claims element “communicates new data associated with an existing security policy ... instructs the plurality of security engines to replace an existing security policy with the new security policy”, is referred in the copending application claims as “accessing a new security policy ...plurality of security engines processing at least a portion of the new security policy ...and switching, after each of the plurality of security engine is ready to begin using the new security policy, each of the plurality of security engines to the new rules substantially concurrently”. It would have been obvious to one having ordinary skill in the art to recognize that communicating new data and associating it with an existing security policy is equivalent to accessing a new security policy and switching to the new rules concurrently.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

7. Claims 1 – 32 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over the amended claims 1 – 60 of copending Application No. 10/456,606. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 32 correspond to the amended claims of 1 – 60 of the copending application claims, except in the instant claims element “communicates new data associated with an existing security policy”, is referred in the copending application claims as “security service configured to monitor in real time the security-related information from the plurality of sources, the security service receiving automatic updates ... performing actions to protect the system based on the security related information”. It would have been obvious to one having ordinary skill in the art to recognize that communicating new data and associating it with an existing security policy is equivalent to identifying and updating the security settings and protecting the system based on the security-related information.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

8. Claims 1 – 32 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 8 – 22 and 34 – 37 of copending Application No. 10/456,093. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 32 correspond to the claims of 8 – 22 and 34 – 37 of the copending application claims, except in the instant claims element “communicates new

data associated with an existing security policy”, is referred in the copending application claims as “installing new filter ... into the policy engine .. comparing the new filter ... and notifying ... about the new filter”. It would have been obvious to one having ordinary skill in the art to recognize that communicating new data and associating it with an existing security policy is equivalent to identifying and processing new filter and further installing the new filter (taking action if the new data corresponds to the existing policy and updating the new security policy).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

9. Claims 1 – 32 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 158 of copending Application No. 10/411,876. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 32 correspond to the claims of 1 – 158 of the copending application claims, except in the instant claims element “communicates new data associated with an existing security policy”, is referred in the copending application claims as “a group policy management program and set of program interfaces operating on group policy related data and communicating with a directory service that is associated with the group policy related data to perform the requested operation”. It would have been obvious to one having ordinary skill in the art to recognize that communicating new data and associating it with an existing security policy is equivalent to managing and communicating group policy (security policy).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1 – 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 – 32 recite “first group of functions”, “second group of functions”, “first function”, “second function”, “third function”, “fourth function”, “fifth function” and “sixth function”. However, no actual definition for these functions has been recited in the claims.

Applicant is advised to amend the claims to clearly state these functions when filing response. Examiner will broadly interpret these functions as instructions to the security engines to modify existing security policy.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1 – 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Ko et al. (U.S. Patent Number 6,789,202).

12. As per Claims 1 and 21, Ko teaches, “a first group of functions related to communicating a new security policy to a plurality of security engines, wherein each of the plurality of security engines is configured to replace an existing security policy with the new security policy; and a second group of functions related to communicating an indication of each security engine's readiness to implement the new security policy” (Fig. 2, 3; Summary and Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

13. As per Claims 14 and 27, Ko teaches, “a first function that communicates a new security policy to the plurality of security engines; a second function that identifies whether each of the plurality of security engines is prepared to apply the new security policy; and a third function that instructs each of the plurality of security engines to implement the new security policy after determining that all of the security engines are prepared to apply the new security policy” (Fig. 2, 3; Summary and Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

14. As per Claim 2, Ko teaches, “wherein the first group of functions includes a method that instructs each of the plurality of security engines to delete the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

15. As per Claim 3, Ko teaches, “wherein the first group of functions includes a method that initializes a particular security engine” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

16. As per Claim 4, Ko teaches, “wherein the first group of functions includes a method that instructs each of the plurality of security engines to implement the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

17. As per Claim 5, Ko teaches, “wherein the first group of functions further comprises a method that communicates new data associated with an existing security policy to at least one of the plurality of security engines” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

18. As per Claim 6, Ko teaches, “wherein the first group of functions further comprises a method that communicates configuration information to at least one of the plurality of security engines” (Column 5 lines 5 – 25 and Column 6 line 19 – Column 7 line 22).

19. As per Claim 7, Ko teaches, “wherein the second group of functions includes a method that indicates whether a particular security engine has implemented the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

20. As per Claim 8, Ko teaches, “wherein the second group of functions further comprises a method that retrieves updated data associated with a particular security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

21. As per Claim 9, Ko teaches, “wherein the second group of functions further comprises a method that communicates new data identified by one of the plurality of

security engines to a security agent” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

22. As per Claim 10, Ko teaches, “wherein the second group of functions further comprises a method that allows one of the plurality of security engines to query a user of a system containing the plurality of security engines” (Column 5 line 5 – 20 and Column 6 line 19 – Column 7 line 22).

23. As per Claim 12, Ko teaches, “wherein at least one of the plurality of security engines implements a firewall application” (Column 6 line 3 – 17 and Column 6 line 19 – Column 7 line 22).

24. As per Claim 13, Ko teaches, “wherein the plurality of security engines implement the new security policy after all security engines have indicated a readiness to implement the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

25. As per Claim 15, Ko teaches, “a fourth function that causes each of the plurality of security engines to delete the new security policy if at least one of the plurality of security engines is unable to apply the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

26. As per Claim 16, Ko teach, “a fourth function related to communicating event information identified by a first security engine to the other security engines” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

27. As per Claim 17, Ko teach, “a fourth function related to communicating security-related information identified by a first security engine to an event manager” (Column 5 line 19 – 28 and Column 6 line 19 – Column 7 line 22).

28. As per Claim 19, Ko teaches, “wherein at least one of the plurality of security engines is associated with a first type of security attack” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

20. As per Claim 22, Ko teaches, “wherein the security-related information identifies a type of security attack” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

30. As per Claim 23, Ko teaches, “calling one or more fourth functions to facilitate communicating a revised security policy to the first security engine” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

31. As per Claim 24, Ko teaches, “calling one or more fourth functions to facilitate communicating configuration information to the first security engine” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

32. As per Claim 25, Ko teaches, “calling one or more fourth functions to facilitate instructing the first security engine and the second security engine to implement the security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

33. As per Claim 26, Ko teaches, “calling one or more fourth functions to facilitate communicating a revised security policy to the first security engine” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

34. As per Claim 28, Ko teaches, “means for exposing a fourth function that communicates a new security policy to the plurality of security engines; and means for exposing a fifth function that instructs the plurality of security engines to replace an existing security policy with the new security policy (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

35. As per Claim 31, Ko teaches, “wherein the security-related event is an unauthorized attempt to access a storage device” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

36. As per Claim 32, Ko teaches, “means for exposing a fourth function that notifies the event manager that a particular security engine has finished processing another function call” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

37. As per Claim 18, Ko teaches, “wherein the event manager communicates the security-related information to at least one of the plurality of security engines” (Column 5 line 19 – 28 and Column 6 line 19 – Column 7 line 22).

38. As per Claim 20, Ko teaches, “wherein at least one of the plurality of security engines is associated with a second type of security attack” (Column 6 lines 3 – 17 and Column 6 line 19 – Column 7 line 22).

37. As per Claim 29, Ko teaches, “means for exposing a sixth function that instructs the plurality to security engines to delete the new security policy if at least one of the plurality of security engines cannot implement the new security policy” (Column 4 line 51 – Column 5 line 4 and Column 6 line 19 – Column 7 line 22).

Allowable Subject Matter

38. Claims 11 and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Ko et al. does not disclose, teach or suggest “at least one of the plurality of security engines implements an antivirus service” and “the security-related event is detection of a virus”.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
October 26, 2007.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


10,27,07